12. *Kutsenko A.* Metrical properties of self-dual bent functions // Des. Codes Cryptogr. 2020. V. 88. No. 1. P. 201–222.
13. *Kutsenko A.* The group of automorphisms of the set of self-dual bent functions // Cryptogr. Commun. 2020.
14. *Куценко А. В.* О множестве расстояний Хэмминга между самодуальными бент-функциями // Прикладная дискретная математика. Приложение. 2016. № 9. С. 29–30.
15. *Куценко А. В.* О некоторых свойствах самодуальных бент-функций // Прикладная дискретная математика. Приложение. 2018. № 11. С. 44–46.
16. *Куценко А. В.* Изометричные отображения множества всех булевых функций в себя, сохраняющие самодуальность и отношение Рэлея // Прикладная дискретная математика. Приложение. 2019. № 12. С. 55–58.
17. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. No. 1. P. 1–10.
18. *MacWilliams F. J. and Sloane N. J. A.* The Theory of Error-Correcting Codes. Amsterdam, New York, Oxford, North-Holland, 1983. 782 p.
19. *Коломеец Н. А., Павлов А. В.* Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–20.
20. *Облаухов А. К.* О метрическом дополнении подпространств булева куба // Дискретный анализ и исследование операций. 2016. Вып. 23. № 3. С. 93–106
21. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press, Elsevier, 2015. 230 p.
22. *Tokareva N.* Duality between bent functions and affine functions // Discrete Math. 2012. V. 312. No. 3. P. 666–670.
23. *Марков А. А.* О преобразованиях, не распространяющих искажения // Избранные труды. Т. II. Теория алгорифмов и конструктивная математика, математическая логика, информатика и смежные вопросы. М.: МЦНМО, 2003. С. 70–93.
24. *Tokareva N. N.* The group of automorphisms of the set of bent functions // Discrete Math. Appl. 2010. V. 20. No. 5. P. 655–664.
25. *Danielsen L. E., Parker M. G., and Solé P.* The Rayleigh quotient of bent functions // LNCS. 2009. V. 5921. P. 418–432.

УДК 519.7 DOI 10.17223/2226308X/13/6

КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА НЕКОТОРЫХ КОМПОЗИЦИЙ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ

Е. С. Липатова

Рассматриваются три класса обратимых векторных булевых функций, таких, что каждая их координатная функция существенно зависит от заданного числа переменных. Приведены результаты экспериментального исследования криптографических свойств композиций функций из этих классов.

Ключевые слова: *векторная булева функция, нелинейность, алгебраическая иммунность, дифференциальная равномерность.*

Обозначим через $\mathcal{F}_n$ множество всех подстановок на $\mathbb{F}_2^n$ и будем рассматривать следующие подклассы функций из $\mathcal{F}_n$:

1) $\mathcal{K}_n$ — функции, полученные из тождественной подстановки с помощью n независимых транспозиций [1];

2) $\mathcal{S}_{n,k}$ — функции вида $F = (f_1, \ldots, f_n)$, где $(f_1, \ldots, f_k) \in \mathcal{K}_k$ и $f_i(x_1, \ldots, x_n) = x_i \oplus \oplus\, g_i(x_1, \ldots, x_{i-1})$, g_i — произвольные булевы функции, существенно зависящие от $k-1$ переменных, $i = k+1, \ldots, n$, $k \leqslant n$ [2, 3];
3) пусть $k|n$; $s = n/k$; $\mathcal{P}_{n,k}$ — функции $F = (f_1, \ldots, f_n)$, где $f_{tk+i}(x_1, \ldots, x_n) = g_i^{(t+1)}(x_{tk+1}, \ldots, x_{(t+1)k})$, $t = 0, \ldots, s-1$ и $i = 1, \ldots, k$; $\left(g_1^{(j)}, \ldots, g_k^{(j)}\right) \in \mathcal{K}_k$, $j = 1, \ldots, s$.

Приведём определения некоторых криптографических характеристик функций $F = (f_1 \ldots f_n) : \mathbb{F}_2^n \to \mathbb{F}_2^n$ [4–6].

Компонентой функции F называется булева функция $vF = v_1 f_1 \oplus \ldots \oplus v_n f_n$, где $v = v_1 \ldots v_n \in \mathbb{F}_2^n \setminus \{0^n\}$; 0^n — нулевой вектор длины n.

Нелинейностью $N(F)$ и *компонентной алгебраической иммунностью* $\mathrm{AI}_{\mathrm{comp}}(F)$ функции F называются минимальные нелинейность и алгебраическая иммунность её компонент соответственно:

$$N(F) = \min_{v \in \mathbb{F}_2^m \setminus \{0^m\}} N(vF), \quad \mathrm{AI}_{\mathrm{comp}}(F) = \min_{v \in \mathbb{F}_2^m \setminus \{0^m\}} \mathrm{AI}(vF).$$

Для векторов $a, b \in \mathbb{F}_2^n$ обозначим $\delta_F(a,b) = |\{x \in \mathbb{F}_2^n : F(x) \oplus F(x \oplus a) = b\}|$. *Показателем дифференциальной равномерности* функции F называется

$$\delta_F = \max_{a \neq 0^n, b} \delta_F(a,b).$$

Проведено экспериментальное исследование этих характеристик, а также алгебраической степени для некоторых композиций функций от 3–10 переменных. Нелинейность, алгебраическая иммунность, дифференциальная равномерность вычислялись по алгоритмам, описанным в [7]; алгебраическая степень — с помощью преобразования Мёбиуса.

В ходе экспериментов получены следующие результаты:

1) Если в композиции участвует случайная подстановка $F \in \mathcal{F}_n$, то характеристики композиции в среднем совпадают с характеристиками функции F. Это можно объяснить тем, что при композиции любой подстановки со случайной равновероятно выбранной равномерное распределение сохраняется [8].
2) Композиция H функции $F \in \mathcal{K}_n$ с функцией $G \in \mathcal{S}_{n,k} \cup \mathcal{P}_{n,k}$ (в любом порядке), можно сказать, берёт наилучшие свойства обоих классов:
   а) $\deg H$ и $\mathrm{AI}_{\mathrm{comp}}(H)$ сохраняются, как у функции F;
   б) δ_H принимает значения, приблизительно равные δ_F, если $G \in \mathcal{S}_{n,k}$, и δ_G, если $G \in \mathcal{P}_{n,k}$;
   в) $N(H) \approx N(G)$.
3) При композиции функций F и G из одного класса, $\mathcal{K}_n$ или $\mathcal{P}_{n,k}$, все рассмотренные свойства в общем ухудшаются:
   а) δ_H принимает худшее значение 2^n, а нелинейность — значение 0 (хотя очень редко получаются значения лучше, чем у исходных функций);
   б) $\mathrm{AI}_{\mathrm{comp}}(H)$ принимает значения 1 или 2 (у исходных функций всегда 2);
   в) $\deg H$ часто равна 1 (редко — как у исходных функций).
4) Про композиции функций из разных классов $\mathcal{S}_{n,k}$ и $\mathcal{P}_{n,k}$ и композиции функций одного класса $\mathcal{S}_{n,k}$ нельзя однозначно сказать о поведении свойств функций:
   а) $\deg H$ часто улучшается;
   б) $\mathrm{AI}_{\mathrm{comp}}(H)$ принимает значения 1 или 2 (те же значения, что и у функций класса $\mathcal{S}_{n,k}$);

в) δ_H в первом случае принимает значения, приблизительно равные δ функций классов $\mathcal{P}_{n,k}$ (очень редко получаются значения лучше или хуже), а во втором случае сохраняется значение 2^n (как у функций класса $\mathcal{S}_{n,k}$);

г) $N(H)$ в обоих случаях может принимать разные значения, в основном они лучше, чем наихудшие значения у функций, используемых в композициях.

ЛИТЕРАТУРА

1. *Pankratova I. A.* Construction of invertible vectorial Boolean functions with coordinates depending on given number of variables // Материалы Междунар. науч. конгресса по информатике: Информационные системы и технологии. Республика Беларусь, Минск, 24–27 окт. 2016. Минск: БГУ, 2016. С. 519–521.
2. *Agibalov G. P.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. № 38. С. 57–65.
3. *Панкратова И. А.* Об обратимости векторных булевых функций // Прикладная дискретная математика. Приложение. 2015. № 8. С. 35–37.
4. *Carlet C.* Vectorial Boolean Functions for Cryptography. Cambridge: Cambridge University Press, 2010. 93 p.
5. *Canteaut A.* Lecture Notes on Cryptographic Boolean Functions. Paris: Inria, 2016. 48 p.
6. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 55–64.
7. *Киселева Н. М., Липатова Е. С., Панкратова И. А., Трифонова Е. Е.* Алгоритмы вычисления криптографических характеристик векторных булевых функций // Прикладная дискретная математика. 2019. № 46. С. 78–87.
8. *Кнут Д.* Искусство программирования. Т. 2. Получисленные алгоритмы. М.: Вильямс, 2007. 832 с.

УДК 519.7 DOI 10.17223/2226308X/13/7

КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА ОРТОМОРФИЗМОВ[1]

Ю. П. Максимлюк

Рассмотрены взаимно однозначные отображения $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, называемые ортоморфизмами, такие, что отображения $G(x) = F(x) \oplus x$ также являются взаимно однозначными. Они используются в схеме Лая — Месси в качестве перемешивающего элемента между раундами, а также для построения криптографически стойких S-блоков. Исследованы основные криптографические свойства: нелинейные характеристики и дифференциальная равномерность. Выявлено, что ортоморфизмы от малого числа переменных не устойчивы к линейному и дифференциальному криптоанализам.

Ключевые слова: *ортоморфизм, таблица линейного преобладания, таблица дифференциалов.*

В симметричной криптографии часто используются отображения множества $\mathbb{Z}_2^n$, состоящего из двоичных наборов длины n, на себя. В частности, в [1] в шифрах FOX (IDEA NXT), использующих схему Лая — Месси, предлагается использовать отображение, называемое ортоморфизмом.

[1]Работа выполнена при поддержке Математического центра в Академгородке (г. Новосибирск), соглашение с Министерством науки и высшего образования Российской Федерации № 075-15-2019-1613, и Лаборатории криптографии JetBrains Research.